78 – Agosto 2006

Que a senha seja forte até a chegada da biometria

A biometria ainda não é uma realidade para a grande maioria dos usuários em todo o mundo. Seja por questões de custo, seja pela baixa popularização do método e de seus dispositivos ou ainda pela natural demora do ciclo de absorção de novas idéias, enquanto a biometria não se torna uma realidade temos que garantir que a velha senha continue nos protegendo.

É evidente a lista de vantagens da biometria, baseadas em "o que você é", em relação á senha, baseada em "o que você tem". A começar pelo fato de que não se pode esquecer nem tão pouco emprestar a íris, o polegar ou a voz, por exemplo. Ao mesmo tempo, quando se está fazendo uso deles, ninguém poderá simplesmente copiá-los ao vê-lo manuseando e desta forma, o processo de autenticação se torna mais robusto.
Todavia não se pode esquecer que todo novo controle de segurança traz consigo novas vulnerabilidades, que neste caso está associada à disponibilidade. Imagine por um instante um executivo em viagem sendo requisitado a acessar e aprovar um documento em caráter emergencial através de um sistema informatizado, mas impossibilitado de se autenticar pessoalmente. Neste caso, sem haver uma outra pessoa igualmente autorizada, como contingência, o processo estaria parado até que houvesse a autenticação forte do usuário. Este tipo de problema não inviabiliza o método, mas revela a necessidade de se projetar cenários e buscar alternativas para adequá-los ao requerimento do nível de segurança.

Voltando portanto à realidade da senha...se é mesmo com ela que ainda teremos que conviver por algum tempo, que ao menos seja forte o bastante para nos fornecer proteção. E apesar de tê-la chamado de velha anteriormente, o usuário precisa mesmo é mantê-la jovem, compatível com o bem protegido e ainda atualizada em relação ao poder da computação. Na prática, com a evolução da microinformática e o aumento exponencial do poder de processamento dos computadores, antiga senha forte de 6 caracteres numéricos, por exemplo, é hoje considerada brincadeira de criança para os mais novos softwares quebradores de senha.
Baseado neste contexto destacam-se algumas dicas conhecidas do que se deve e não se deve fazer com a senha.

O que fazer com a sua senha	**O que não fazer com a sua senha**
Misture letras em maiúsculo e minúsculo além de números e caracteres especiais.	Não utilize nenhuma variação da senha de seu login de rede.
Utilize caracteres alfanuméricos com pontuação quando suportado pelo sistema.	Não use seu nome, apelido ou suas iniciais como base para criação da senha.
Utilize mais letras em maiúsculo do que apenas na primeira posição.	Não utilize nenhuma palavra de dicionário, mesmo que em outra língua, acrônimos e abreviações.
Use pelo menos 6 caracteres, aumentando preferencialmente para 8.	Não utilize nenhuma outra informação sobre você que possa ser facilmente obtida.

	Incluindo nome de animais de estimação, números de telefone, marca de automóveis, nome de ruas, por exemplo.
Forme uma senha aparentemente randômica, sem que ela tenha um significado lógico.	Não utilize senhas formadas somente por números ou caracteres alfanuméricos, quando o sistema permitir.
Forme uma senha que se possa digitar rapidamente sem ter que olhar o teclado.	Não utilize datas ou a combinação de datas como base para formação de senhas.
Troque sua senha regularmente. A freqüência deve acompanhar a criticidade do bem protegido.	Não utilize seqüências de teclas do teclado.
Troque obrigatoriamente sua senha se suspeitar de algum vazamento ou do comprometimento de seu sigilo.	Não utilize exemplos de senhas mencionados em livros sobre segurança ou qualquer outra literatura por mais forte que possa parecer.
Memorize a senha, mas se tiver de escrever, prefira escrever apenas algo que o faça lembrá-la.	Não escreva a senha em papeis, notas, calendários ou em ambientes online se outros usuários puderem acessar.
Evite associações quando formar sua senha. Forte é senha que não se consegue descobrir por dedução.	Não compartilhe contas de acesso e senhas e não revele sua senha para ninguém.

Se for criativo forme uma senha extraindo a primeira letra de cada palavra de uma pequena frase e mescle com a pontuação. Mas se a criatividade lhe faltar, apele para os softwares geradores de senhas aleatórias. Mais importante mesmo é ter em mente que, de acordo com a estimativa do CERT – *Computer Emergency Response Team*, 80% de todos os problemas de segurança de rede são causados por senhas fracas.

Estou certo de que estas medidas deverão ser dosadas de acordo com o grau de sensibilidade da informação protegida e que, em alguns casos, nem todas as dicas serão aplicáveis por limitações do ambiente. Entretanto, a adoção de algumas delas já tornará seu acesso mais seguro e o manterá vivo e respirando até que finalmente a biometria se popularize.

Marcos Sêmola *é Consulting Business Development da multinacional Atos Origin em Londres, Consultor Sênior em Gestão de Segurança da Informação, profissional certificado CISM – Certified Information Security Manager pelo ISACA, BS7799 Lead Auditor pelo BSI, Membro da ISACA, ISSA, IBGC, CSI e membro fundador do IISP – Institute of Information Security Professionals of London. Professor da FGV – Fundação Getúlio Vargas, Pós Graduando em Negociação e Estratégia pela London School, MBA em Tecnologia Aplicada, Pós Graduado em Marketing e Estratégia de Negócios, Bacharel em Ciência da Computação, autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed. Campus, autor de outras duas obras ligadas à gestão da informação pelas editoras Saraiva e Pearsons e premiado pela ISSA como SecMaster®, Profissional de Segurança da Informação de 2003 Setor Privado e 2004*

Desenvolvimento de Mercado, sendo membro da comissão julgadora em 2005. Visite www.semola.com.br ou contate marcos@semola.com.br